„Absent precise guidance from the founding era“

Gastautor 2014-10-09T10:17:58

von PAOLO RAMADORI

Der Oberste Gerichtshof der Vereinigten Staaten hat sich in der Entscheidung *Riley v. California* vom 25. Juni erstmals nachdrücklich zu einem Problem der digitalisierten Lebenswelt geäußert. Die Durchsuchung der Daten, die auf einem Handy gespeichert sind, greife besonders intensiv in die Privatsphäre seines Benutzers ein.

Das Leben auf der Straße ist nicht leicht

Riley war in San Diego wegen der Nummernschilder an seinem Lexus von der Polizei angehalten worden; die Zulassung des Autos war abgelaufen. Eine nachfolgende Personenkontrolle ergab dann, dass auch *Rileys* Fahrerlaubnis suspendiert worden war. Der Beamte beschloss, den Wagen zu beschlagnahmen. Zu diesem Zweck untersuchte er ihn vor der Sicherstellung auf vorhandene Schäden. Unter der Motorhaube entdeckte er zwei geladene Pistolen, die in einer Socke versteckt waren. Mit *Rileys* anschließender Verhaftung fingen seine Schwierigkeiten an.

Der Polizist durchsuchte ihn und warf dabei auch einen Blick in sein Smartphone und die darin gespeicherten Nachrichten. Er bemerkte das Kürzel „CK“, das szenekundigen Beamten als Abkürzung für „Crip Killers“ geläufig ist. Es deutet auf die Feindschaft zwischen den berüchtigten Straßengangs „Crips“ und „Bloods“ hin. Eine systematische Auswertung des Telefons durch einen Spezialisten erhärtete den Verdacht, dass Riley ein Mitglied der „Bloods“ sein könnte. Im Speicher fanden sich nämlich Fotos, auf denen er sich per Handzeichen zu der Bande bekannte.

Als verhängnisvoll erwies sich allerdings ein anderes Fundstück: Auf einer weiteren Aufnahme posierte Riley bewaffnet vor einem Straßenkreuzer, der den Ermittlern bekannt vorkam. Von dem Oldsmobile aus war einige Wochen zuvor ein fahrendes

Auto beschossen worden. Eine ballistische Untersuchung ordnete schließlich die damals am Tatort gefundenen Patronenhülsen den beiden Waffen zu, die *Riley* in seinem Auto versteckt hatte. Die Beweise wurden in einem Strafprozess gegen ihn verwertet und trugen zu seiner Verurteilung wegen versuchten Mordes sowie verschiedener Körperverletzungs-, Waffen- und Verkehrsdelikte bei.

„Data is different“

Der Supreme Court stellt fest, dass die gespeicherten Daten eines Mobiltelefons nicht ohne richterlichen Beschluss gesichtet werden können. Die Ausnahmeregelung *incident to lawful arrest* lässt sich nicht auf diese Konstellation übertragen; insoweit ist *Riley* in seinem Recht auf Privatsphäre aus dem vierten Verfassungszusatz verletzt. Insbesondere für Smartphones müssten andere Regeln gelten als für analoge Gebrauchsgegenstände, wie zum Beispiel Zigarettenschachteln.

Der vierte Zusatzartikel der US-Verfassung schützt die Person, die Wohnung, die Urkunden und das Eigentum des Einzelnen durch einen Richtervorbehalt vor willkürlicher Durchsuchung und Beschlagnahme; unter Anderem in dieser Vorschrift wird das verfassungsmäßige Recht auf Privatsphäre (*privacy*) verortet. Verletzungen des *fourth amendment* schlagen sich im Strafprozessrecht in einem Beweisverwertungsverbot nieder (*fruit of the poisonous tree doctrine*).

Das *common law* kennt allerdings einige Befreiungen von dem Richtervorbehalt; in ihrem Anwendungsbereich verletzt auch eine Durchsuchung, der kein Beschluss von Seiten der Justiz vorausgegangen ist, nicht die Rechte aus dem vierten Verfassungszusatz. Zu diesen Ausnahmen zählt auch die Durchsuchung einer Person und ihrer räumlichen Umgebung bei einer rechtmäßigen Verhaftung ([search] *incident to lawful arrest*); sie dient der Sicherheit der verhaftenden Beamten und beugt der Zerstörung oder Verdunklung von Beweismitteln vor. Entwickelt wurde die Regel in den Entscheidungen *Chimel* (1969) und *Robinson* (1973). Besonders die zweite Entscheidung kommt für den Fall *Riley* als Präjudiz in Frage: Sie befindet die Durchsuchung einer Zigarettenschachtel, die bei einer Verkehrskontrolle mit anschließender Leibesvisitation entdeckt wurde, für verfassungsmäßig.

Sind die beiden Sachverhalte aber überhaupt vergleichbar? Ein Smartphone unterscheidet sich in der Vielfalt und Wirkkraft seiner Funktionen erheblich von den Gegenständen, die ein Mensch in den siebziger Jahren am Körper tragen konnte; eine „mechanische“ Subsumtion der *incident-to-lawful-arrest*-Regel verbietet sich nach Auffassung des Obersten Gerichtshofes. Lässt sich stattdessen eine reflektierte Anwendung auf moderne Mobiltelefone begründen? Die Verfassungsgeber haben dazu, wie der Gerichtshof verdeutlicht, keine Hilfestellung geliefert. Der Präsident des Gerichts, Justice Roberts, bewertet die Regel deswegen im Lichte einer Abwägung (*balancing*) der berührten Verfassungsgüter neu. *Robinson* wird nicht nur auf seine tatsächliche, sondern anschließend auch auf seine normativ-verfassungsrechtliche Vergleichbarkeit mit dem Fall *Riley* hin überprüft. Sowohl im Falle der Zigarettenschachtel als auch im Fall des Smartphones stehen nämlich der Schutz des Beamten und das staatliche Strafverfolgungsinteresse gegen die Privatsphäre des Verhafteten.

Auch diese – in der US-Rechtsprechung noch eher ungewöhnliche – Güterabwägung spricht jedoch gegen eine Anwendung der *incident-to-lawful-arrest*-Ausnahme. Das Interesse des Staates, die Beweismittel zu sichern und die verhaftenden Beamten zu schützen, kann durch die Informationen, die auf einem Smartphone abgelegt sind, nur in Ausnahmefällen gefährdet werden. Konstellationen, in denen Daten die Sicherheit eines Beamten bedrohen, sind kaum denkbar. Eine Fernlöschung des Telefonspeichers kann abgewendet werden, indem das Handy abgeschaltet oder in einer abgeschirmten Tasche (*faraday bag*) verstaut wird. Die Privatsphäre des Benutzers ist durch die Durchsuchung dagegen besonders stark betroffen.

Neuerungen in Verfassungsrecht und *common-law*-Methode

Die besondere Eingriffstiefe der Auswertung der gespeicherten Informationen ist die Kernaussage der Entscheidung. *Roberts* begründet sie mit der schieren Menge an Daten, die ein handelsübliches Smartphone speichern kann, mit der Variationsbreite an verfügbaren Informationstypen, deren Kombination umfassende Rückschlüsse über Leben und Persönlichkeit des Benutzers erlaubt, und schließlich damit, dass die gespeicherten Daten zeitlich bis zum Kaufdatum des Gerätes zurückreichen können. Unter den verschiedenen Informationsarten finden sich überdies neuartige Datensätze, wie etwa Bewegungsprofile. Eine besondere Relevanz erhalte das Problem dadurch, dass 90% der US-Bürger ein solches Gerät benutzten und stets bei sich führten.

Das Gericht passt implizit auch die Präjudizmethode des *common law* an den technischen Fortschritt an. Die Digitalisierung des Alltags ändert unsere Lebenswelt so tiefgreifend, dass in den betreffenden Konstellationen vom Grundsatz der *stare decisis* abgewichen werden kann. Nach dieser Regel sind rechtliche Aussagen, die in Präzedenzfällen aufgestellt wurden, nur dann im zu entscheidenden Fall maßgeblich, wenn dieser auf tatsächlicher Ebene hinreichend mit dem Präjudiz vergleichbar ist. Das Gericht hat hier eine tatsächliche Vergleichbarkeit mit *Robinson* verneint. Damit hätte nach bisheriger Praxis festgestellt werden müssen, dass die Entscheidung als Präjudiz nicht einschlägig ist. Dennoch fährt *Roberts* aber darin fort, eine Geltung der in *Robinson* begründeten *incident-to-lawful-arrest*-Regel zu diskutieren: An die Stelle tatsächlicher Vergleichbarkeitsüberlegungen tritt die Abwägung (*balancing*) der betroffenen verfassungsrechtlichen Gesichtspunkte.

Durch diese Anpassung der Fallrechtsmethode könnte die Entscheidung zuletzt auch auf vordigitale Sachverhalte zurückwirken. Mithilfe des *balancing*-Ansatzes ließe sich nämlich auch die Durchsuchung von analogen Informationsträgern wie Notiz- oder Adressbüchern neu bewerten. Die Eingriffstiefe ist zwar bei der Sichtung eines Notizbuches geringer als bei der Durchsuchung eines Telefonspeichers; den rechtfertigenden Gesichtspunkten kommt allerdings in derartigen Fällen gar kein Gewicht zu. Schließlich können auch auf Papier niedergelegte Informationen den Beamten nicht gefährden. Analoge Datenträger lassen sich außerdem nicht aus der Ferne löschen.

Ein Vorgeschmack?

Das Urteil wird in den USA als verfassungsrechtlicher Sprung in das digitale Zeitalter angesehen. Zwar hatte sich der Oberste Gerichtshof schon früher zu moderner Informationstechnologie geäußert. Im Fall *Jones* (2012) hatten die Behörden ein Gerät am Auto eines Verdächtigen angebracht, das seine Ortung per GPS ermöglichte. Die Mehrheit der Richter hatte den Fall aber eher konservativ mithilfe der *trespass*-Regel gelöst, die auf das physische Eindringen in das Fahrzeug mit der Absicht abstellt, persönliche Informationen zu erlangen.

In der *Riley*-Entscheidung berücksichtigt und betont das Gericht hingegen die Neuartigkeit der Eingriffe durch technische Überwachungsmöglichkeiten. Die Begründung ist eng am Gegenstand des Mobiltelefons und an der Verhaftungssituation entwickelt, weist aber dennoch weit über beides hinaus. Dies gilt zunächst für die Zentralaussage zur Eingriffstiefe, die implizit den verfassungsrechtlichen Schutz der Privatsphäre auf einen digitalen Massenspeicher erstreckt. Darüber hinaus lehnt das Gericht auch den Vorschlag, eine Sichtung einzelner Bereiche des Telefons zu erlauben, als praxisfern ab; eine begrenzte Durchsuchung digitaler Speichermedien wird mit der Auswertung aller verfügbaren Daten gleichgesetzt.

Sämtliche alternativen Lösungsvorschläge und Argumente der Regierung werden sorgfältig gewürdigt und widerlegt; auch ist die Entscheidung einstimmig ergangen. Möglicherweise wird der Gerichtshof sich bald weiterer Fragen der Digitalisierung annehmen, etwa des *cloud computing* und nicht zuletzt der Überwachungspraxis der NSA.
